UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,291	08/16/2001	Marinus Frans Kaashoek	12221-005001	3137

26161 7590 03/25/2005

FISH & RICHARDSON PC
225 FRANKLIN ST
BOSTON, MA 02110

EXAMINER	
JACKSON, JENISE E	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 03/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/931,291	KAASHOEK ET AL.	
	Examiner	Art Unit	
	Jenise E Jackson	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3,5-9,12-16,18,19,21,24 and 25* is/are rejected.

7)☒ Claim(s) *2,4,10,11,17,20,22,23,26 and 27* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date ~~03072005~~. 12 23 04
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1, 3, 5-6, 9, 12-13, 18-19, 21 are rejected under 35 U.S.C. 102(b) as being anticipated by Messmer.

3. As per claims 1, 9, 18, 21, Messmer teaches a central control center(i.e. Counterpane data center)(see lines 26-28) to coordinate thwarting attacks(see lines 1-20), coordinating thwarting attacks is taught in Messmer, because Messmer teaches that the data center monitors network traffic to determine if the customers network is under attack. Messmer teaches a victim data center, because Messmer teaches that outsourcing intrusion detection, one company that does this is Counterpane, Counterpane monitors customers network(see lines 12-15), the customers network is the victim data center. Messmer teaches a communication device(i.e. probe/black box)(see lines 17-26) to receive data from a plurality of monitors(see lines 23-26), dispersed through the network(see lines 23-27), the monitors sending data collected from the network over a hardened redundant network(see lines 23-28), Messmer teaches a hardened redundant network because the data collected is sent in encrypted form to the central control center(see lines 23-28). Messmer teaches the redundant network being a physically separate network from the network that the plurality of monitors collect data from, because the plurality of monitors are on the customers network(12-26), the central control center has its own network, that is in California or

Virginia, where the data from the monitors is collected and sent to the data center(see lines 26-28). Messmer teaches a computer system that includes a process that executes on the computer system to analyze the data from the plurality of monitors to determine network traffic statistics that can identify malicious network traffic(see lines 28-32).

4. As per claim 3, Messmer teaches wherein the data analyzed by the control center is collected statistical information about network flows(see lines 29-30).

5. As per claim 5, Messmer teaches wherein the control center is a hardened site, because the data collected is sent in encrypted form to the central control center(see lines 23-28). Messmer teaches the redundant network being a physically separate network from the network that the plurality of monitors collect data from, because the plurality of monitors are on the customers network(12-26), the central control center has its own network, that is in California or Virginia, where the data from the monitors is collected and sent to the data center(see lines 26-28).

6. As per claim 6, Messmer teaches wherein the monitors include gateways that are disposed at the victim data center and data collectors that are disposed in the network(see lines 12-25), the analysis process executed on the control center analyzes data from gateways and data collectors dispersed throughout the network(see lines 26-30).

7. As per claims 12, 19, Messmer teaches receiving and analyzing are performed by a control center coupled to the data collectors via the hardened, redundant network(see lines 12-28).

8. As per claim 13, Messmer teaches wherein plurality of monitoring devices(see lines 13-26); are data collectors dispersed throughout the network and at least one gateway device that is

disposed adjacent the victim site to protect the victim (see lines 6-26), and wherein analyzing includes analyzing at a control center data from the at least one gateway and the data collectors dispersed throughout the network(see lines 26-30).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 7-8, 14-16, 24-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Messmer in view of Hill et al.

11. As per claims 7, 14, 24 Messmer does not disclose classifying attack. However, Hill et al. does disclose classifying attacks(see col. 5, lines 66-67, col. 6, lines 1-18). It would have been obvious to one of ordinary skill in the art at the time of the invention to include Hill et al. classifying attacks within Messmer, because classifying attacks displays attack information in a usable and quickly interpretable form to a network manager while minimizing the loading on the computer(see col. 2, lines 45-50 of Hill et al.). Therefore, by classifying attacks provides a network manager with knowledge of the severity and overall nature of the attack(see col. 2, lines 53-60 of Hill et al.).

12. As per claims 8, 15, 25 same motivation as above. Hill et al. discloses wherein the classes of attack are denoted as low-grade with spoofing, low-grade without spoofing and high-grade whether spoofing or non-spoofing(see fig. 3, sheet 3, fig. 7, sheet 6).

13. As per claim 16, Messmer teaches sending requests to gateways to send data pertaining to an attack to the control center(see lines 14-27).

13. Claims 2, 4, 10-11, 17, 20, 22-23, 26-27 are objected to as being rejected on base claims. The reasons why these claims are objected to is because the control center of prior art does not eliminate block or request the victim center to set up filters. The prior art of record monitors for intrusions, the center monitors and gives the victim center ways in which to handle the attacks.

Response to Amendment

14. New art has been applied to claims in response to Applicant's arguments. Therefore, arguments presented by Applicant in regards to Porras are moot.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E Jackson whose telephone number is (571) 272-3791. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

March 8, 2005

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100